

Blind quantum computation for Alice who does only measurements

Tomoyuki Morimae¹ and Keisuke Fujii²

¹ IRCS, Tokyo Institute of Technology, 2-12-1 Ookayama, Meguro-ku, Tokyo 152-8550, Japan

² Graduate School of Engineering Science, Osaka University, Toyonaka, Osaka 560-8531, Japan

(Dated: January 20, 2012)

Blind quantum computation is a secure quantum computing protocol which enables Alice who does not have sufficient quantum technology to ask Bob to perform quantum computation on Bob's fully-fledged quantum computer in such a way that Bob cannot learn anything about Alice's input, output, and algorithm. In previous proposals, Alice needs to have a device which generates quantum states, such as single-photon states. Here we show that Alice who does only measurements, such as the polarization measurements with a threshold detector, can perform the blind quantum computation. In several experimental setups, such as optical systems, the measurement of a state is much easier than the generation of a single-qubit state. Therefore our protocols can ease Alice's burden. Furthermore, the security of our protocols is device independent in the sense that Alice does not need to trust her measurement device. Finally, the security of our protocols is based on the no-signaling principle, which is more fundamental than quantum physics.

Introduction.— Our future quantum computing will be in the style of the “cloud quantum computing”, since only limited number of groups, such as governments and huge industries, will be able to possess scalable quantum computers. How can a server of the cloud quantum computing assure the security of a client's privacy in the cloud quantum computing? The concept of the blind quantum computation [1–8] provides the solution. Blind quantum computation is a secure quantum computing protocol which enables a client (Alice) who has only a classical computer or a primitive quantum device which is not sufficient for universal quantum computation to ask a server (Bob) to perform her quantum algorithm on his fully-fledged quantum computer without leaking any Alice's privacy (i.e., which algorithm Alice wants to run, which value Alice inputs, and what is the output of the computation) to Bob [1–8]. For classical computation, Feigenbaum [9] introduced the notion of “computing with encrypted data”, and showed that for some functions f , an instance x can be efficiently encrypted into $z = E_k(x)$ in such a way that Alice can recover $f(x)$ efficiently from k and $f(z)$ computed by Bob. Moreover Abadi, Feigenbaum and Killian showed that no **NP**-hard function can be computed blindly if unconditional security is required, unless the polynomial hierarchy collapses at the third level [10]. Even restricting the security condition to be only computational, the question of the possibility of blind computing, also known as fully homomorphic encryption, remained open for 30 years [11].

The first example of blind quantum computation was proposed by Childs [1] where the quantum circuit model was adopted, and the register state was encrypted with quantum one-time pad scheme [12] so that Bob who performs quantum gates learns nothing about information in the quantum register. In this method, however, Alice needs to have a quantum memory and the ability to perform the SWAP gate. The protocol proposed by Ar-

righi and Salvail [2] is that for the calculation of certain classical functions, i.e., not the universal quantum computation, and it requires Alice to prepare and measure multi-qubit entangled states. Furthermore, it is cheat-sensitive, i.e., Bob can gain information if he does not mind being caught. Finally, in their protocol, Bob knows the unitary which Alice wants to implement. Aharonov, Ben-Or and Eban's protocol [4] requires a constant-sized quantum computer with memory.

On the other hand, in 2009, Broadbent, Fitzsimons and Kashefi [3] proposed a new blind quantum computation protocol which uses the one-way model [13–16]. In their protocol, all Alice needs are a classical computer and a primitive quantum device, which emits randomly rotated single-qubit states. In particular, Alice does not require any quantum memory and the protocol is unconditionally secure. Recently, this protocol has been experimentally demonstrated in an optical system [7]. Furthermore, this innovative protocol has inspired several new other protocols which can enjoy robust blind quantum computation. In Ref. [5], two protocols which enable blind measurement-based quantum computation on the Affleck-Kennedy-Lieb-Tasaki (AKLT) state [17, 18] have been proposed. In Ref. [8], a protocol of the blind topological measurement-based quantum computation [19–21] has been proposed. Due to the topological protection, it is fault-tolerant [19–21]. The error threshold of the blind topological model has been shown to be comparable to that of the original [19, 20] (i.e., non-blind) topological quantum computation [8].

Before starting the main part of this paper, let us quickly review the protocol of Ref. [3]. In this protocol, Alice and Bob share a classical channel and a quantum channel. The protocol runs as follows: (1) Alice prepares randomly-rotated single-qubit states $\{|\theta_j\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta_j}|1\rangle)\}_{j=1}^N$, where $\theta_j \in \mathcal{A} \equiv \{\frac{k\pi}{4} | k = 0, 1, \dots, 7\}$ is a random angle, and sends them to Bob through the quantum channel. (2) Bob creates a certain two-

dimensional graph state, which is called the brickwork state [3], from $\{|\theta_j\rangle\}_{j=1}^N$ by applying the CZ gates. (3) Alice calculates the measurement angle on her classical computer, and sends it to Bob through the classical channel. (4) Bob performs the measurement in that angle, and returns the measurement result to Alice. They repeat (3)-(4) until the computation is finished. If Bob is honest, Alice obtains the correct answer of her desired quantum computation [3]. If Bob is not cooperative, the correctness of the final output is no longer guaranteed. However, it can be shown that whatever evil Bob does, Bob cannot learn anything about Alice's input, output, and algorithm [3]. (An intuitive understanding of the security of this protocol is as follows. Let us assume that Alice wants Bob to measure a particle of the graph state in the angle ϕ . If Alice directly sends ϕ to Bob, Bob knows ϕ , and therefore Bob can gain some information about Alice's algorithm. Therefore, Alice sends $\delta = \phi + \theta + r\pi$ to Bob, where $r \in \{0, 1\}$ is a random number which comes from a certain technical reason which we do not explain here [3]. Since the particle to be measured is pre-rotated by θ in the above process (1), the particle is effectively measured in the angle $\phi + r\pi$, when Bob does the measurement in the angle δ . The effect of $r\pi$ is just the flip of the measurement result. In this way, Alice can have Bob do the measurement in the angle ϕ without allowing Bob to know the value of ϕ .)

The motivation of the blind quantum computation is to enable Alice, who does not have any sophisticated technology and deep knowledge, to perform universal quantum computation. Therefore, there are two important goals. One is to make Alice's device as classical as possible, since Alice is not expected to have any expensive laboratory which can maintain the coherence of complicated quantum experimental setups. The other is to exempt Alice from the precise verification of her device, since Alice is not expected to have enough technology and knowledge to verify her device. Such a verification is important since she might buy the device from a company which is under the control of Bob, and therefore the device might not work as Alice expects. For example, if Alice is supposed to send a single-photon to Bob, Alice must confirm that more than two identical photons are not sent to Bob, since otherwise Bob might be able to gain some information by using, e.g., the photon-number-splitting (PNS) attack [22–25]. In Ref. [6], a first step to the first goal, namely making Alice's device more classical, was achieved. They proposed an ingenious protocol of the blind quantum computation in which what Alice needs to prepare are not single-photon states but coherent states. Since coherent states are considered to be more classical than single-photon states, their protocol allows Alice's device to be more classical.

In this paper, we show that Alice who has only a measurement device can perform the blind quantum computation. We propose three protocols each of which has its

own advantages. In several experimental setups, such as quantum optical systems, the measurement of a state, e.g., the polarization measurement of photons with a threshold detector, is much easier than the generation of a single-qubit state, such as a single-photon state. Therefore, our results achieve the above mentioned first goal, namely making Alice's device more classical. As we will see later, our protocols can cope with the particle loss in the quantum channel and the measurement inefficiencies, which also means that our protocols allow Alice's device to be more classical. Furthermore, our protocols also achieve the second goal: the security of our protocols is “device independent” [26] in the sense that Alice does not need to trust her measurement device. Finally, we will see that the security of our protocols is based on the no-signaling principle [27], which is more fundamental than quantum physics [27].

Protocol 1.— Our first protocol runs as follows: (1) Bob prepares a resource state of measurement-based quantum computation. Any resource state can be used for this purpose. For example, the two-dimensional cluster state [13–15], the three-dimensional cluster state for the topological quantum computation [19–21], the thermal equilibrium states of a nearest-neighbour two-body Hamiltonian with spin-2 and spin-3/2 particles [28] or solely with spin-3/2 particles [29] at a finite temperature for the topological measurement-based quantum computation, resource states for the quantum computational tensor network [30–32], the one-dimensional or two-dimensional AKLT states [18, 33, 34], the tri-cluster state [35], and states in the Haldane phase [36]. (2) Bob lets Alice know which resource state he has. (3) Bob sends a particle of the resource state to Alice through the quantum channel. (4) Alice does a measurement on the particle. They repeat (3)-(4) until the computation is finished.

Obviously, at the end of the computation, Alice obtains the correct answer of her desired quantum computation if Bob is honest, since what Alice and Bob did is nothing but a usual measurement-based quantum computation. (It is something like the following story: Alice and Bob are in the same laboratory. The preparation and the maintenance of the resource state, which are boring routines, are done by poor Bob, whereas the most exciting part of the measurement-based quantum computation, namely the measurements and the collection of data are done by his boss Alice. Somehow, there is no communication between them.)

It is also easy to understand that whichever states evil Bob prepares instead of the correct resource state, and whichever states evil Bob sends to Alice, Bob cannot learn anything about Alice's information, since Alice does not send any signal to Bob and therefore because of the no-signaling principle [27] Bob cannot gain any information about Alice by measuring his system [37]: If Alice could transmit some information to Bob by measur-

ing her system, it contradicts to the no-signaling principle [39]. (Note that we assume there is no unwanted leakage of information from Alice's laboratory. For example, Bob cannot bug Alice's laboratory. It is the standard assumption in the quantum key distribution [40].) In Appendix A, we give the mathematical proof of the security of Protocol 1 based on the no-signaling principle.

Protocol 1 has four advantages. First, no random-number generator is required for Alice. This is advantageous since it is not easy to generate completely random numbers, and the random-number generator might be provided by a company under the control of Bob. Second, the security of the protocol is "device independent" in the sense that Alice does not need to trust her measurement device, since whatever Alice does, Bob cannot gain any information about Alice's computation as long as there is no unwanted leakage of information from Alice's laboratory, which is the standard assumption in quantum key distribution [40]. Third, the proof of the security is intuitive and very simple, and it is based on the no-signaling principle [27], which is more fundamental than quantum physics [27]. (Even if quantum physics is violated in a future, Protocol 1 survives as long as the no-signaling principle holds.) Finally, any model of measurement-based quantum computation (such as the cluster model [13–15], the AKLT models [18, 33, 34], and the topological model [19–21], etc.) can be directly changed into a blind model: Bob has only to let Alice do measurements. (On the other hand, in Ref. [5], many complicated procedures are required to make the AKLT measurement-based quantum computation blind.) Since no modification is required to make a model blind, the advantage of a model is preserved when it is changed into a blind model. For example, an advantage of doing the measurement-based quantum computation on the AKLT states is that the quantum computation is protected by the energy gap of a physically natural Hamiltonian [18, 33, 34]. If the AKLT model is used in Protocol 1, Bob who prepares and maintains the resource AKLT state can enjoy that advantage, i.e., Bob's state is protected by the energy gap. This is also the case for the models of Refs. [28, 29]: If these models are used in Protocol 1, Bob can enjoy the advantage of these models, i.e., Bob does not need to keep his state in the ground state; His state is allowed to be the equilibrium state at a finite temperature.

A disadvantage of Protocol 1 is that the quantum channel between Alice and Bob must not be too lossy. (Throughout this paper, "the channel loss" includes the detection inefficiency of Alice's device, since the detection inefficiency behaves like the channel loss.) On the other hand, in the previous protocols [3, 5, 7, 8] where Alice sends randomly rotated particles to Bob, the high loss rate of the quantum channel is not crucial, since if Bob does not receive a particle due to the loss in the quantum channel, Bob has only to ask Alice to again generate and send another state with another random

angle. One way of overcoming that disadvantage of Protocol 1 is to use a model which can cope with the particle loss. For example, it was shown in Ref. [41] that the topological measurement-based quantum computation [19–21] can cope with the heralded particle loss if the loss probability is below the threshold. If Bob uses this model, Alice and Bob can perform Protocol 1 without suffering from the particle loss as long as the loss rate of the quantum channel between Alice and Bob (and that of Alice's device) is below the loss threshold calculated in Ref. [41].

Protocol 2.— If the channel loss rate is too high, we can use the following protocol, Protocol 2, which runs as follows: (1) Bob creates the Bell pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and sends a half of it to Alice through the quantum channel. By using the classical channel, Bob lets Alice know that he sent the particle. (2) If Alice does not receive the particle, because of the channel loss, Alice asks Bob to try again, and goes back to (1). (3) If Alice receives the particle, she generates a random number $\theta \in \mathcal{A}$, and measures the particle in the basis $\{\frac{1}{\sqrt{2}}(|0\rangle \pm e^{-i\theta}|1\rangle)\}$. After Alice's measurement, Bob's state is, from Alice's view point, $|\theta\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\theta}|1\rangle)$ if her measurement result is $m = 0$, and $|\theta + \pi\rangle = \frac{1}{\sqrt{2}}(|0\rangle - e^{i\theta}|1\rangle)$ if her measurement result is $m = 1$. However, from Bob's view point, it is the completely-mixed state $\frac{1}{2}I$, since Bob does not know Alice's measurement result. (4) They repeat (1)–(3) until Bob has N particles. (5) From these N particles, Bob creates the brickwork state [3] or the three-dimensional cluster state for the topological measurement-based quantum computation [19–21]. For the former, the blind protocol of Ref. [3] is used, and for the latter, the blind protocol of Ref. [8] is used.

Obviously, if Bob is honest, the correct blind quantum computation is possible. On the other hand, if evil Bob prepares some another state instead of the Bell pair, and sends some of them to Alice, the correct quantum computation is no longer guaranteed. However, we can show that whichever states evil Bob prepares, and whichever states evil Bob sends to Alice, Bob cannot gain any information about Alice's input, output, and algorithm [42]. A proof of the security of Protocol 2 is given in Appendix B. Note that, unlike Protocol 1, Protocol 2 does not require a quantum channel with low loss rate, since if the half of a Bell pair is lost in the channel, Alice has only to ask Bob to generate a Bell pair and to send a half of the Bell pair again. There are three disadvantages in Protocol 2. First, Protocol 2 can be used only for some class of models of measurement-based quantum computation, such as the two-dimensional cluster model [13–15] and the topological model [19–21], where the entangling operations which create the resource state commute with the random prerotation of each particle. Second, Alice needs a random number generator. Third, the proof of the security is no longer based on the no-signaling prin-

ciple, since Alice sends classical messages δ to Bob [3, 8].

Protocol 3.— Surprisingly, we can modify Protocol 2 in such a way that Alice does not need any random number generator and that the security is based on the no-signaling principle. How can we do that? First, in order to respect the no-signaling principle, Alice cannot send any classical message which is related to her algorithm. Therefore, Alice must measure the half of the Bell pair in a specific (not random) angle which is related to her algorithm. Second, Bob’s measurements must be done always in the same angle, since otherwise Bob can gain some information about Alice’s computational angles. It is exciting to notice that we have a similar situation in a completely different field, namely, the fault-tolerant quantum computation on the one-way model [46]. There, only Pauli-basis measurements are allowed since the Calderbank-Shor-Steane (CSS) codes support transversal measurements only for the Pauli basis [47, 48]. In order to perform non-Clifford gates, the magic states [49] are injected. These facts suggest that if (1) Bob sends a half of a Bell pair to Alice, (2) Alice measures the half of the Bell pair in a specific angle, and (3) after Alice’s measurement Bob injects his half of the Bell pair into his resource state, then universal quantum computation could be possible even if Bob does the measurements in a fixed basis. In fact, we can do that in Protocol 3, which runs as follows: (1) Bob creates the Bell pair $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and sends a half of it to Alice through the quantum channel. By using the classical channel, Bob lets Alice know that he sent the particle. (2) If Alice does not receive the particle due to the channel loss, Alice asks Bob to try again, and goes back to (1). (3) If Alice receives the particle, she measures it in the basis $\{\frac{1}{\sqrt{2}}(|0\rangle \pm e^{-i\theta}|1\rangle)\}$, where θ is a certain angle (not a random angle) determined by the algorithm which Alice wants to run. ($\theta = 0, \pi/2$ for a Clifford gate, and $\theta = \pi/4$ for a non-Clifford gate. For details, see Appendix C.) (4) Bob couples the half of the Bell pair which he has to his state by using the CZ gate, and does the measurement in the $\{|+\rangle, |-\rangle\}$ basis. (For details, see Appendix C.) (5) Bob returns the measurement result to Alice through the classical channel. (6) They repeat (1)-(5) until the

computation is finished. As is shown in Appendix C, if Bob is honest Alice can obtain the correct answer of her desired quantum computation by appropriately taking θ ’s. Also, in Appendix D, it is shown that whichever states evil Bob prepares and whichever states evil Bob sends to Alice, Bob cannot learn anything about Alice’s information. Intuitive understanding of the security of Protocol 3 is as follows. In Protocol 3, Alice sometimes sends the message “I did not receive the particle. So send it again.” to Bob through the classical channel. Because of this fact, one might think that the no-signaling assumption can no longer be applied. However, we can still consider that the situation is “effectively no-signaling”, since what Alice sends to Bob is obviously nothing to do with Alice’s input, output, and algorithm, and therefore effectively, there is no signal transmission from Alice to Bob. In other words, there is no meaningful signal transmission from Alice to Bob. Therefore, it is reasonable that in such an “effectively no-signaling” situation, Bob cannot gain any information about Alice’s computation by measuring his system.

Discussion.— In this paper, we have proposed three protocols of blind measurement-based quantum computation for Alice who can do only measurements, such as the polarization measurement with a threshold detector. In quantum optics, for example, the state measurement is much easier than the single-qubit state generation. Therefore our scheme makes Alice more classical than the previous protocols [3, 5, 8] in certain experimental setups, such as optical systems. In the protocol of Ref. [6], Bob is required to perform the non-demolition photon-number measurement, which is not easy with the current technology. In our protocols, on the other hand, Bob is not required to have such an additional high technology. Finally, there is a way of detecting evil Bob: Alice can randomly choose some subsystem of the resource state and measure the stabilizer operators in order to check whether Bob creates a correct resource state.

KF is supported by MEXT Grant-in-Aid for Scientific Research on Innovative Areas 20104003. TM thanks V. Dunjko and E. Kashefi for valuable discussions about the security of blind quantum computation.

Appendix A

We assume that the initial state of the computation is the standard state $|0\dots 0\rangle$, and the preparation of the input state is included in the computational part. Therefore, what Alice wants to hide are the computation angles of the measurement-based quantum computation and the final output of the computation. Intuitively, a protocol is blind if Bob, given all the classical and quantum information during the protocol, cannot learn anything about Alice’s computational angles and the output [3, 5, 6].

Definition: *In this paper, we call a protocol is blind if*

- (B1) *The conditional probability distribution of Alice’s computational angles, given all the classical information Bob can obtain during the protocol, and given the measurement results of any POVMs which Bob may perform on his system at any stage of the protocol, is equal to the a priori probability distribution of Alice’s computational*

angles, and

(B2) The conditional probability distribution of the final output of Alice's algorithm, given all the classical information Bob can obtain during the protocol, and given the measurement results of any POVMs which Bob may perform on his system at any stage of the protocol, is equal to the a priori probability distribution of the final output of Alice's algorithm.

■

Theorem 1: Protocol 1 satisfies (B1).

Proof: Let A be the random variable which represents Alice's measurement angles, and B be the random variable which represents the type of the POVM which Bob performs on his system. Let M_B be the random variable which represents the result of Bob's POVM. The two-party system is called no-signaling [27] from Alice to Bob iff

$$P(M_B = m_B | A = a, B = b) = P(M_B = m_B | A = a', B = b),$$

for all m_B , a , a' , and b . Then,

$$\begin{aligned} P(A = a | B = b, M_B = m_B) &= \frac{P(M_B = m_B | A = a, B = b)P(A = a, B = b)}{P(B = b, M_B = m_B)} \\ &= \frac{P(M_B = m_B | A = a, B = b)P(A = a | B = b)P(B = b)}{P(B = b, M_B = m_B)} \\ &= \frac{P(M_B = m_B | A = a', B = b)P(A = a' | B = b)P(B = b)}{P(B = b, M_B = m_B)} \\ &= P(A = a' | B = b, M_B = m_B). \end{aligned}$$

This means that Bob cannot learn anything about Alice's measurement angles. ■

Theorem 2: Protocol 1 satisfies (B2).

Proof: Let O be the random variable which represents the output of Alice's algorithm, and B be the random variable which represents the type of the POVM which Bob performs on his system. Let M_B be the random variable which represents the result of Bob's POVM. Alice can change the output of her algorithm by changing the input. (For example, since what is implemented in the quantum computation is a unitary operation, two input states which are orthogonal with each other become two mutually-orthogonal output states.) Because of the no-signaling principle,

$$P(M_B = m_B | O = o, B = b) = P(M_B = m_B | O = o', B = b)$$

for all m_B , o , o' , and b . Then,

$$\begin{aligned} P(O = o | B = b, M_B = m_B) &= \frac{P(M_B = m_B | O = o, B = b)P(O = o, B = b)}{P(B = b, M_B = m_B)} \\ &= \frac{P(M_B = m_B | O = o, B = b)P(O = o | B = b)P(B = b)}{P(B = b, M_B = m_B)} \\ &= \frac{P(M_B = m_B | O = o', B = b)P(O = o' | B = b)P(B = b)}{P(B = b, M_B = m_B)} \\ &= P(O = o' | B = b, M_B = m_B). \end{aligned}$$

Therefore, Bob cannot learn anything about the output of Alice's algorithm. ■

Appendix B

Theorem 3: Protocol 2 satisfies (B1).

Proof: Let us define

$$\begin{aligned} \Delta &\equiv (\Delta_1, \dots, \Delta_N), \\ \Phi &\equiv (\Phi_1, \dots, \Phi_N), \\ \Theta &\equiv (\Theta_1, \dots, \Theta_N), \\ R &\equiv (R_1, \dots, R_N), \end{aligned}$$

where $\Delta_j, \Theta_j, \Phi_j \in \mathcal{A} \equiv \{\frac{k\pi}{4} | k = 0, 1, \dots, 7\}$ and $R_j \in \{0, 1\}$ are random variables, corresponding to the angles sent by Alice to Bob, Alice's measurement angles, Alice's secret computational angles, and the hidden binary parameters, respectively. From the construction of the protocol [3, 8], the following relation is satisfied:

$$\Delta_j = \Phi_j + \Theta_j + S_j\pi + R_j\pi \pmod{2\pi},$$

where $S_j \in \{0, 1\}$ is Alice's j th measurement result. Let $\{\Pi_j\}_{j=1}^m$ be a POVM which Bob may perform on his system. Let $O \in \{1, \dots, m\}$ be the random variable corresponding to the result of the POVM. Let T be the random variable which represents Alice's message about the channel loss. Bob's knowledge about Alice's computational angles is given by the conditional probability distribution of $\Phi = (\phi_1, \dots, \phi_N)$ given $O = j$, $T = t$, and $\Delta = (\delta_1, \dots, \delta_N)$:

$$P(\Phi = \vec{\phi} \mid O = j, \Delta = \vec{\delta}, T = t),$$

where $\vec{\phi} = (\phi_1, \dots, \phi_N)$ and $\vec{\delta} = (\delta_1, \dots, \delta_N)$. From Bayes' theorem, we have

$$\begin{aligned} P(\Phi = \vec{\phi} \mid O = j, \Delta = \vec{\delta}, T = t) &= \frac{P(O = j \mid \Phi = \vec{\phi}, \Delta = \vec{\delta}, T = t)P(\Phi = \vec{\phi}, \Delta = \vec{\delta}, T = t)}{P(O = j, \Delta = \vec{\delta}, T = t)} \\ &= \frac{P(O = j \mid \Phi = \vec{\phi}, \Delta = \vec{\delta}, T = t)P(\Phi = \vec{\phi})P(\Delta = \vec{\delta}, T = t)}{P(O = j \mid \Delta = \vec{\delta}, T = t)P(\Delta = \vec{\delta}, T = t)} \\ &= P(\Phi = \vec{\phi}) \frac{\text{Tr}(\Pi_j \rho_{\vec{\phi}, \vec{\delta}, t})}{\text{Tr}(\Pi_j \rho_{\vec{\delta}, t})} \\ &= P(\Phi = \vec{\phi}), \end{aligned}$$

where

$$\begin{aligned} \rho_{\vec{\phi}, \vec{\delta}, t} &= \frac{1}{2^N} \sum_{r_1=0}^1 \dots \sum_{r_N=0}^1 \sum_{s_1=0}^1 \dots \sum_{s_N=0}^1 \text{Tr}_A(\rho \bigotimes_{i=1}^N |\delta_i - \phi_i - s_i\pi - r_i\pi\rangle \langle \delta_i - \phi_i - s_i\pi - r_i\pi|) \\ &= \text{Tr}_A(\rho) \end{aligned}$$

and

$$\begin{aligned} \rho_{\vec{\delta}, t} &= \frac{1}{8^N} \sum_{\phi_1 \in \mathcal{A}} \dots \sum_{\phi_N \in \mathcal{A}} \frac{1}{2^N} \sum_{r_1=0}^1 \dots \sum_{r_N=0}^1 \sum_{s_1=0}^1 \dots \sum_{s_N=0}^1 \text{Tr}_A(\rho \bigotimes_{i=1}^N |\delta_i - \phi_i - s_i\pi - r_i\pi\rangle \langle \delta_i - \phi_i - s_i\pi - r_i\pi|) \\ &= \text{Tr}_A(\rho). \end{aligned}$$

■

Theorem 4: *Protocol 2 satisfies (B2).*

Proof: It is easy to confirm that when Bob measures a particle, the register state is one-time padded with $Z^\alpha X^\beta$, where $\alpha, \beta \in \{0, 1\}$ are determined by Bob's previous measurement results.

The values of α and β are unknown to Bob, since $\{r_j\}_{j=1}^N$ are unknown to Bob. We can show that $\{r_j\}_{j=1}^N$ are unknown to Bob as follows.

$$\begin{aligned} P(R = \vec{r} \mid O = j, \Delta = \vec{\delta}, T = t) &= \frac{P(O = j \mid R = \vec{r}, \Delta = \vec{\delta}, T = t)P(R = \vec{r}, \Delta = \vec{\delta}, T = t)}{P(O = j, \Delta = \vec{\delta}, T = t)} \\ &= \frac{P(O = j \mid R = \vec{r}, \Delta = \vec{\delta}, T = t)P(R = \vec{r})P(\Delta = \vec{\delta}, T = t)}{P(O = j \mid \Delta = \vec{\delta}, T = t)P(\Delta = \vec{\delta}, T = t)} \\ &= P(R = \vec{r}) \frac{\text{Tr}(\Pi_j \rho_{\vec{r}, \vec{\delta}, t})}{\text{Tr}(\Pi_j \rho_{\vec{\delta}, t})} \\ &= P(R = \vec{r}) \\ &= \frac{1}{2^N}, \end{aligned}$$

where

$$\begin{aligned}\rho_{\vec{r}, \vec{\delta}, t} &= \frac{1}{8^N} \sum_{\phi_1 \in \mathcal{A}} \dots \sum_{\phi_N \in \mathcal{A}} \sum_{s_1=0}^1 \dots \sum_{s_N=0}^1 \text{Tr}_A(\rho \bigotimes_{i=1}^N |\delta_i - \phi_i - s_i\pi - r_i\pi\rangle \langle \delta_i - \phi_i - s_i\pi - r_i\pi|) \\ &= \text{Tr}_A(\rho).\end{aligned}$$

■

Appendix C

Protocol 3 runs as follows: (1) Bob prepares the Bell pair and sends the half of it to Alice. (2) If Alice does not receive it, she asks Bob to try again, and goes back to (1). (3) If Alice receives the particle, she does the measurement in the

$$\left\{ \frac{1}{\sqrt{2}}(|0\rangle \pm e^{-i\theta}|1\rangle) \right\}$$

basis. How to choose θ will be explained later. After her measurement, Bob has the state

$$Z^a R_\theta |+\rangle,$$

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$, $a \in \{0, 1\}$ is Alice's measurement result, and

$$R_\theta = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}.$$

Note that $R_\theta X = e^{i\theta} X R_{-\theta}$. (4) Bob creates the state

$$CZ_{1,2}(|\psi\rangle_1 \otimes Z^a R_\theta |+\rangle_2),$$

where $CZ_{1,2}$ is the CZ gate between the first and the second qubits and $|\psi\rangle$ is any Bob's state. (5) Bob performs the measurement in the basis $\{|+\rangle, |-\rangle\}$ on the first qubit. Since $Z^a R_\theta$ commutes with $CZ_{1,2}$, Bob obtains

$$Z^a R_\theta X^m H |\psi\rangle_2 \tag{1}$$

if the measurement result is $m \in \{0, 1\}$, where H is the Hadamard gate.

For $\theta = 0$, Eq. (1) becomes

$$Z^a X^m H |\psi\rangle_2.$$

For $\theta = \pi/2$, Eq. (1) becomes

$$\begin{aligned}Z^a R_{\pi/2} X^m H |\psi\rangle_2 &= Z^a X^m R_{(-1)^m \pi/2} H |\psi\rangle_2 \\ &= Z^a X^m Z^m R_{\pi/2} H |\psi\rangle_2 \\ &= Z^{a+m} X^m S H |\psi\rangle_2,\end{aligned}$$

where $S = R_{\pi/2}$.

For $\theta = -\pi/4$, Eq. (1) becomes

$$\begin{aligned}Z^a R_{-\pi/4} X^m H |\psi\rangle_2 &= Z^a X^m R_{(-1)^m \pi/4} H |\psi\rangle_2 \\ &= \begin{cases} Z^a X^m T H |\psi\rangle_2 & (m = 0) \\ Z^a X^m T^\dagger H |\psi\rangle_2 & (m = 1), \end{cases}\end{aligned}$$

where $T = R_{-\pi/4}$.

Note that

$$\begin{aligned}
(PH)(PH)(PH) &= PH, \\
(PH)(PH)(PSH) &= PSH, \\
(PH)(PSH)(PSH) &= PHSHSH = PZS \\
(PH)(PH)(PTH) &= PTH, \\
(PSH)(PH)(PTH) &= PT^\dagger H, \\
(PSH)(PH)(PT^\dagger H) &= PTH, \\
(PH)(PH)(PT^\dagger H) &= PT^\dagger H,
\end{aligned}$$

where P is a Pauli byproduct. (Be careful that different Pauli byproducts are represented by the same character P for simplicity.) This means that the operations

$$\{H, TH, T^\dagger H, SH, S\}$$

can be done deterministically (up to Pauli byproducts) if Alice and Bob repeat the above (1)-(5) three times. Therefore, if we consider the unit cell (Fig. 1), the operations

$$\{I \otimes I, SH \otimes I, STH \otimes I, ST^\dagger H \otimes I, H \otimes I, (CZ)(CNOT)\}$$

can be implemented deterministically up to some Pauli byproducts as is shown in Fig. 2. Note that this set is universal set, since

$$\begin{aligned}
(PSH)(PH) &= PS, \\
(PS)(PSTH)(P'H) &= PT, \\
(PS)(PST^\dagger H)(P''H) &= PT,
\end{aligned}$$

where P' is I or X , and P'' is Z or XZ . As is shown in Fig. 3, the unit cell can be tiled to create the universal two-dimensional graph state which resembles the brickwork state [3].

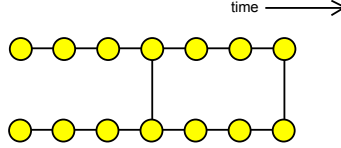


FIG. 1: (Color online.) The unit cell for Protocol 3.

Appendix D

Theorem 5: *Protocol 3 satisfies (B1).*

Proof: Let B be the random variable which represents the type of the POVM which Bob performs on his system, and M_B be the random variable which represents the result of the POVM. Let T be the random variable which represents Alice's message to Bob about the channel loss. Let A be the random variable which represents Alice's measurement angles. Bob's knowledge about Alice's measurement angles is given by the conditional probability distribution of $A = a$ given $B = b$, $M_B = m_B$ and $T = t$:

$$P(A = a \mid B = b, M_B = m_B, T = t).$$

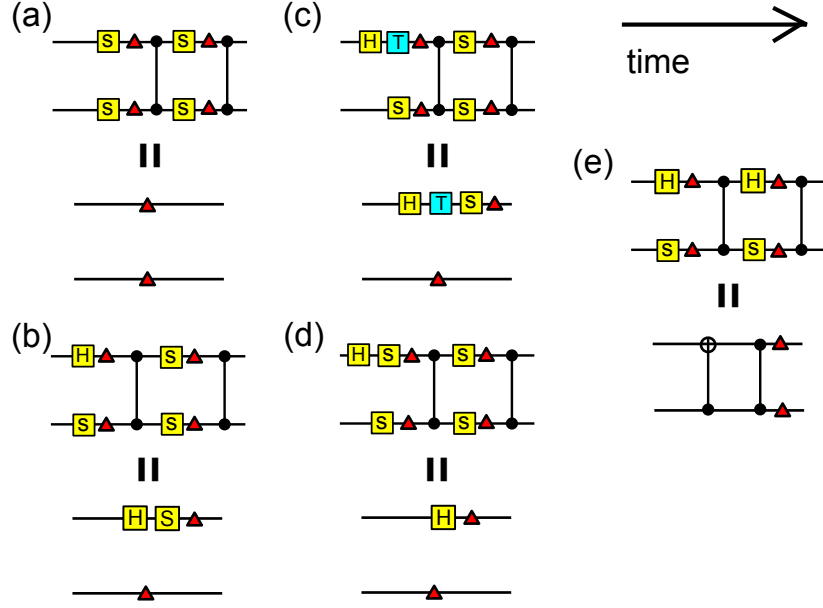


FIG. 2: (Color online.) Operations which can be implemented in the unit cell. Red triangles are Pauli byproducts. In (c), the blue T can be replaced with T^\dagger .

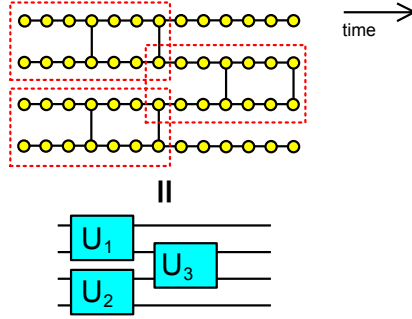


FIG. 3: (Color online.) Tiling for Protocol 3.

From Bayes' theorem, we have

$$\begin{aligned}
 P(A = a \mid B = b, M_B = m_B, T = t) &= \frac{P(M_B = m_B, A = a, B = b, T = t)}{P(B = b, M_B = m_B, T = t)} \\
 &= \frac{P(M_B = m_B, A = a, B = b)P(T = t)}{P(B = b, M_B = m_B, T = t)} \\
 &= \frac{P(M_B = m_B \mid A = a, B = b)P(A = a, B = b)P(T = t)}{P(B = b, M_B = m_B, T = t)} \\
 &= \frac{P(M_B = m_B \mid A = a', B = b)P(A = a', B = b)P(T = t)}{P(B = b, M_B = m_B, T = t)} \\
 &= P(A = a' \mid B = b, M_B = m_B, T = t).
 \end{aligned}$$

■

Theorem 6: *Protocol 3 satisfies (B2).*

Proof: Let B be the random variable which represents the type of the POVM which Bob performs on his system, and M_B be the random variable which represents the result of the POVM. Let T be the random variable which represents Alice's message to Bob about the channel loss. Let O be the random variable which represents the output

of Alice's algorithm. Bob's knowledge about the output of Alice's algorithm is given by the conditional probability distribution of $O = o$ given $B = b$, $M_B = m_B$, and $T = t$:

$$P(O = o \mid B = b, M_B = m_B, T = t).$$

From Bayes' theorem, we have

$$\begin{aligned} P(O = o \mid B = b, M_B = m_B, T = t) &= \frac{P(M_B = m_B, O = o, B = b, T = t)}{P(B = b, M_B = m_B, T = t)} \\ &= \frac{P(M_B = m_B, O = o, B = b)P(T = t)}{P(B = b, M_B = m_B, T = t)} \\ &= \frac{P(M_B = m_B \mid O = o, B = b)P(O = o, B = b)P(T = t)}{P(B = b, M_B = m_B, T = t)} \\ &= \frac{P(M_B = m_B \mid O = o', B = b)P(O = o', B = b)P(T = t)}{P(B = b, M_B = m_B, T = t)} \\ &= P(O = o' \mid B = b, M_B = m_B, T = t). \end{aligned}$$

■

-
- [1] A. Childs, *Quant. Inf. Compt.* **5**, 456 (2005).
- [2] P. Arrighi and L. Salvail, *Int. J. Quant. Inf.* **4**, 883 (2006).
- [3] A. Broadbent, J. Fitzsimons, and E. Kashefi, *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science* 517 (2009).
- [4] D. Aharonov, M. Ben-Or, and E. Eban, *Proceedings of Innovations in Computer Science* 453 (2010).
- [5] T. Morimae, V. Dunjko, and E. Kashefi, arXiv:1009.3486
- [6] V. Dunjko, E. Kashefi, and A. Leverrier, arXiv:1108.5571
- [7] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, arXiv:1110.1381
- [8] T. Morimae and K. Fujii, arXiv:1110.5460
- [9] J. Feigenbaum, *Proceedings of Advances in Cryptography* 477 (1986).
- [10] M. Abadi, J. Feigenbaum, and J. Kilian, *Journal of Computer and System Science* **39**, 21 (1989).
- [11] C. Gentry, *Proceedings of the 41st annual ACM Symposium on Theory of Computing* 169 (2009).
- [12] P. Boykin and V. Roychowdhury, *Phys. Rev. A* **67**, 042317 (2003).
- [13] R. Raussendorf and H. J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001).
- [14] R. Raussendorf, D. E. Browne, and H. J. Briegel, *Phys. Rev. A* **68**, 022312 (2003).
- [15] R. Raussendorf, Ph.D. thesis, Ludwig-Maximilians Universität München, 2003.
- [16] It is insightful to point out here that one great advantage of the measurement-based quantum computation which enables a simple blind protocol is the clear separation between the quantum stage (resource preparation) and the classical stage (measurements and classical-signal feed-forward). In order to see it, let us consider the following story. Alice and Bob are in the same laboratory. Bob prepares the resource state, and he measures a particle. Then Alice hammers Bob, and Bob loses his memory. Bob does the second measurement and again Alice hammers Bob. If they repeat this process until the end of the computation, Alice finally gets the output of the desired quantum computation. However, Bob gets no information about this quantum computation since he loses his memory every time.
- [17] I. Affleck, T. Kennedy, E. H. Lieb, and H. Tasaki, *Comm. Math. Phys.* **115**, 477 (1988).
- [18] G. K. Brennen and A. Miyake, *Phys. Rev. Lett.* **101**, 010502 (2008).
- [19] R. Raussendorf and J. Harrington, *Phys. Rev. Lett.* **98**, 190504 (2007).
- [20] R. Raussendorf, J. Harrington, and K. Goyal, *New J. of Phys.* **9**, 199 (2007).
- [21] R. Raussendorf, J. Harrington, and K. Goyal, *Ann. Phys.* **321**, 2242 (2006).
- [22] B. Huttner, N. Imoto, N. Gisin, and T. Mor, *Phys. Rev. A* **51**, 1863 (1995).
- [23] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, *J. Cryptology* **5**, 3 (1992).
- [24] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, *Phys. Rev. Lett.* **85**, 1330 (2000).
- [25] N. Lütkenhaus, *Phys. Rev. A* **61**, 052304 (2000).
- [26] A. Acin, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *Phys. Rev. Lett.* **98**, 230501 (2007).
- [27] S. Popescu and D. Rohrlich, *Found. Phys.* **24**, 379 (1994).
- [28] Y. Li, D. E. Browne, L. C. Kwek, R. Raussendorf, and T. C. Wei, *Phys. Rev. Lett.* **107**, 060501 (2011).
- [29] K. Fujii and T. Morimae, arXiv:1111.0919, to be published in *Phys. Rev. A* (R)
- [30] D. Gross and J. Eisert, *Phys. Rev. Lett.* **98**, 220503 (2007).
- [31] D. Gross, J. Eisert, N. Schuch, and D. Perez-Garcia, *Phys. Rev. A* **76**, 052315 (2007).
- [32] D. Gross and J. Eisert, *Phys. Rev. A* **82**, 040303(R) (2010).
- [33] A. Miyake, *Ann. Phys.* **326**, 1656 (2011).
- [34] T. C. Wei, I. Affleck, R. Raussendorf, *Phys. Rev. Lett.* **106**, 070501 (2011).
- [35] X. Chen, B. Zeng, Z. Gu, B. Yoshida, and I. L. Chuang, *Phys. Rev. Lett.* **102**, 220501 (2009).
- [36] A. Miyake, *Phys. Rev. Lett.* **105**, 040501 (2010).
- [37] It is interesting to note that measurement-based quantum computation is the sequence of teleportations [38],

and therefore if Alice does not send her measurement result, Bob's state is the completely-mixed state.

- [38] F. Verstraete and J. I. Cirac, Phys. Rev. A **70**, 060302(R) (2004).
- [39] The security of Protocol 1 is easily understood from the following logic. In Protocol 1, Alice can choose two strategies: (1) Doing the correct measurements. (2) Just discarding all particles sent from Bob. Let ρ_i ($i = 1, 2$) be Bob's state after Alice finishing the strategy (i). Of course, $\rho_1 = \rho_2$, since otherwise Alice can transmit some message to Bob. And, obviously, ρ_2 does not contain any information about Alice's input, output and algorithm, since no quantum computation was performed. Therefore ρ_1 does not contain any information about Alice's computation.
- [40] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
- [41] S. D. Barrett and T. M. Stace, Phys. Rev. Lett. **105**, 200502 (2010).
- [42] The relation between the protocol of Ref. [3] and Protocol 2 reminds us of the well-known duality relation [43] between the BB84 protocol [44] and the E91 protocol [45] in quantum key distribution. In fact, we have a similar situation: In the protocol of Ref. [3] there is a possibility that Alice's device emits more than two identical photons. In order to prohibit Bob from exploiting these extra photons, Alice needs some additional procedure, such as Ref. [6]. On the other hand, in Protocol 2 Alice does not need to do that: She has only to block all quantum information flow from Alice to Bob, which is much easier than the single-photon verification.
- [43] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
- [44] C. H. Bennett and G. Brassard, Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore India, 175 (1984).
- [45] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
- [46] K. Fujii and K. Yamamoto, Phys. Rev. A **81**, 042324 (2010).
- [47] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
- [48] A. M. Steane, Phys. Rev. Lett. **77**, 793 (1996).
- [49] S. Bravyi and A. Kitaev, Phys. Rev. A **71**, 022316 (2005).